



#3

Patent
Attorney's Docket No. 019952-157

THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of)
Hideyuki TORII) Group Art Unit: 2167
Application No.: 09/819,814) Examiner: Unassigned
Filed: March 29, 2001)
For: ASSETS MANAGEMENT METHOD)
AND SYSTEM)

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior application in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed:

Japanese Patent Application No. 2000-199276

Filed: June 30, 2000.

In support of this claim, enclosed is a certified copy of the prior foreign application. This application is referred to in the oath or declaration. Acknowledgment of receipt of this certified copy is requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: July 9, 2001

By: William Charles RN 30811, Esq.
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620



(Translation of the front page
of the priority document of
Japanese Patent Application
No. 2000-199276)

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of
the following application as filed with this Office.

Date of Application : June 30, 2000

Application Number : Patent Application
2000-199276

Applicant(s) : NUMERICAL TECHNOLOGIES KABUSHIKI KAISHA

May 11, 2001

Commissioner,

Patent Office

Kouzo OIKAWA

Certification Number 2001-3037570



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 6月30日

出 願 番 号

Application Number:

特願2000-199276

出 願 人

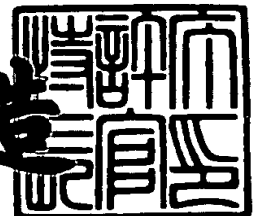
Applicant(s):

ニューメリカルテクノロジーズ株式会社

2001年 5月11日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3037570

【書類名】 特許願

【整理番号】 2000P0901

【提出日】 平成12年 6月30日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/00

【発明の名称】 資産管理方法及びそのシステム

【請求項の数】 12

【発明者】

【住所又は居所】 東京都文京区本郷3丁目4番5号ボア本郷4階 ニューメリカルテクノロジーズ株式会社内

【氏名】 鳥居 秀行

【特許出願人】

【住所又は居所】 東京都文京区本郷3丁目4番5号ボア本郷4階

【氏名又は名称】 ニューメリカルテクノロジーズ株式会社

【代表者】 鳥居 秀行

【代理人】

【識別番号】 100076428

【弁理士】

【氏名又は名称】 大塚 康徳

【電話番号】 03-5276-3241

【選任した代理人】

【識別番号】 100101306

【弁理士】

【氏名又は名称】 丸山 幸雄

【電話番号】 03-5276-3241

【選任した代理人】

【識別番号】 100115071

【弁理士】

【氏名又は名称】 大塚 康弘

【電話番号】 03-5276-3241

【手数料の表示】

【予納台帳番号】 003458

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 資産管理方法及びそのシステム

【特許請求の範囲】

【請求項 1】 資産に関する入力データを計算してリスク管理及び収益管理のデータを作成するリスク収益管理装置に、利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理手段を設けて、使用者の資源へのアクセスを管理し、

不特定多数の利用者による、ネットワークを介した前記リスク収益管理装置へのアクセスを可能とすることを特徴とする資産管理方法。

【請求項 2】 前記履歴認証管理手段は、利用者又は管理対象資産に基づいてリスク収益管理装置の資源を利用する権限を付与することを特徴とする請求項 1 記載の資産管理方法。

【請求項 3】 前記利用者とリスク収益管理装置との間でネットワークを介して伝送されるデータは、機密性に応じて暗号化されることを特徴とする請求項 1 記載の資産管理方法。

【請求項 4】 資産に関する入力データを計算してリスク管理及び収益管理のデータを作成するリスク収益管理装置と、ネットワークを介して前記リスク収益管理装置にアクセスする利用者端末とを含む資産管理システムであって、

前記リスク収益管理装置に、利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理手段を設けて、使用者の資源へのアクセスを管理し、

不特定多数の利用者による、ネットワークを介した前記リスク収益管理装置へのアクセスを可能とすることを特徴とする資産管理システム。

【請求項 5】 前記履歴認証管理手段は、利用者又は管理対象資産に基づいてリスク収益管理装置の資源を利用する権限を付与することを特徴とする請求項 4 記載の資産管理システム。

【請求項 6】 前記利用者とリスク収益管理装置との間でネットワークを介して伝送されるデータは、機密性に応じて暗号化されることを特徴とする請求項 4 記載の資産管理システム。

【請求項 7】 利用者又は管理対象資産毎の入出力データを格納及び検索す

るデータ管理手段と、

該入力データを処理し出力データを得る計算処理手段と、

利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理手段と、

フロー制御とデータ暗号化とデータ圧縮展開を行うネットワーク接続管理手段とを備えることを特徴とするリスク収益管理装置。

【請求項 8】 前記履歴認証管理手段は、利用者又は管理対象資産に基づいてリスク収益管理装置の資源を利用する権限を付与することを特徴とする請求項 7 記載のリスク収益管理装置。

【請求項 9】 前記ネットワーク接続管理手段は、前記利用者とリスク収益管理装置との間でネットワークを介して伝送されるデータは、機密性に応じて暗号化することを特徴とする請求項 7 記載のリスク収益管理装置。

【請求項 10】 資産に関する入力データを計算してリスク管理及び収益管理のデータを作成するリスク収益管理装置を制御する制御プログラムをコンピュータ読み取り可能に記憶する記憶媒体であって、

前記制御プログラムが、

利用者又は管理対象資産毎の入出力データを格納及び検索するデータ管理プログラムと、

該入力データを処理し出力データを得る計算処理プログラムと、

利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理プログラムと、

フロー制御とデータ暗号化とデータ圧縮展開を行うネットワーク接続管理プログラムとを含むことを特徴とする記憶媒体。

【請求項 11】 前記履歴認証管理プログラムは、利用者又は管理対象資産に基づいてリスク収益管理装置の資源を利用する権限を付与するステップを含むことを特徴とする請求項 10 記載の記憶媒体。

【請求項 12】 前記ネットワーク接続管理プログラムは、前記利用者とリスク収益管理装置との間でネットワークを介して伝送されるデータは、機密性に応じて暗号化するステップを含むことを特徴とする請求項 10 記載の記憶媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【産業上の利用分野】

本発明は、地理的に分散した利用者及び管理対象資産のデータを対象として、効率的かつ安全な資産のリスク管理及び収益管理を可能とする資産管理方法及びそのシステムに関するものである。

【 0 0 0 2 】

【従来の技術】

従来のこの種の方法及びシステムでは、資産のリスク管理及び収益管理を可能とするために、管理対象資産の入力データ管理部と、該入力データから計算結果を得る計算処理部と、該計算結果の格納及び検索を行う出力データ管理部と、利用者に実際の機能を提供するユーザインタフェース部とを、1つの一体化したシステムとして構築するか、あるいは相互に緊密にネットワーク接続したシステムとして構築しており、処理できる管理対象資産は小規模であった。

【 0 0 0 3 】

これは、顧客情報や信用情報が含まれるなど機密性の高い金融データが外部に流出する危険を避けるため、同一の企業体内での利用あるいは機密性の低い情報の分析に用途が限定されていたためである。

【 0 0 0 4 】

しかしながら、昨今、データ量が大きな大手事業法人や金融機関規模の資産に対してリスク管理及び収益管理機能を提供することが求められており、その為には、広帯域かつ信頼性の高いネットワーク間通信が必要となる。

【 0 0 0 5 】

この要求を実現するためには、従来のシステムでは、地理的に分散した利用者及び管理対象資産のデータが対象の場合に、インターネット接続に代表されるようなネットワークは、安価な反面、帯域が限定される又は信頼性の乏しいため、利用することが困難であった。

【 0 0 0 6 】

又、従来のシステムでは、バリュー・アット・リスク (V a R)、リスク・リターン分析、ポートフォリオ最適化など、個別の方法論において様々な見解や手

法の相違が含まれるポートフォリオ理論を適用しようとした場合、利用者又は管理対象資産毎に別々の方式や異なる基準を提供することが困難であった。

【0 0 0 7】

更に、従来のシステムでは、持続的な機能向上や改定を行う場合には利用者端末側の装置又はソフトウェアを変更する必要がある、稼動後の機能の変更が難しく、変更をするには維持コストの上昇を招いていた。

【0 0 0 8】

【発明が解決しようとする課題】

本発明は、上記従来の欠点を除去し、地理的に分散した利用者及び管理対象資産のデータを対象にした、安価で融通性に富み、信頼性の高い、効率的かつ安全な資産のリスク管理及び収益管理を可能とする資産管理方法及びそのシステムを提供する。

【0 0 0 9】

【課題を解決するための手段】

上述した課題を解決するために、本発明の資産管理方法は、資産に関する入力データを計算してリスク管理及び収益管理のデータを作成するリスク収益管理装置に、利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理手段を設けて、使用者の資源へのアクセスを管理し、不特定多数の利用者による、ネットワークを介した前記リスク収益管理装置へのアクセスを可能とすることを特徴とする。ここで、前記履歴認証管理手段は、利用者又は管理対象資産に基づいてリスク収益管理装置の資源を利用する権限を付与する。また、前記利用者とリスク収益管理装置との間でネットワークを介して伝送されるデータは、機密性に応じて暗号化される。

【0 0 1 0】

又、本発明の資産管理システムは、資産に関する入力データを計算してリスク管理及び収益管理のデータを作成するリスク収益管理装置と、ネットワークを介して前記リスク収益管理装置にアクセスする利用者端末とを含む資産管理システムであって、前記リスク収益管理装置に、利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理手段を設けて、使用者の資源へのアクセスを管理し

、不特定多数の利用者による、ネットワークを介した前記リスク収益管理装置へのアクセスを可能とすることを特徴とする。ここで、前記履歴認証管理手段は、利用者又は管理対象資産に基づいてリスク収益管理装置の資源を利用する権限を付与する。また、前記利用者とリスク収益管理装置との間でネットワークを介して伝送されるデータは、機密性に応じて暗号化される。

【 0 0 1 1 】

又、本発明のリスク収益管理装置は、利用者又は管理対象資産毎の入出力データを格納及び検索するデータ管理手段と、該入力データを処理し出力データを得る計算処理手段と、利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理手段と、フロー制御とデータ暗号化とデータ圧縮展開を行うネットワーク接続管理手段とを備えることを特徴とする。ここで、前記履歴認証管理手段は、利用者又は管理対象資産に基づいてリスク収益管理装置の資源を利用する権限を付与する。又、前記ネットワーク接続管理手段は、前記利用者とリスク収益管理装置との間でネットワークを介して伝送されるデータは、機密性に応じて暗号化する。

【 0 0 1 2 】

又、本発明に記憶媒体は、資産に関する入力データを計算してリスク管理及び収益管理のデータを作成するリスク収益管理装置を制御する制御プログラムをコンピュータ読み取り可能に記憶する記憶媒体であって、前記制御プログラムが、利用者又は管理対象資産毎の入出力データを格納及び検索するデータ管理プログラムと、該入力データを処理し出力データを得る計算処理プログラムと、利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理プログラムと、フロー制御とデータ暗号化とデータ圧縮展開を行うネットワーク接続管理プログラムとを含むことを特徴とする。ここで、前記履歴認証管理プログラムは、利用者又は管理対象資産に基づいてリスク収益管理装置の資源を利用する権限を付与するステップを含む。又、前記ネットワーク接続管理プログラムは、前記利用者とリスク収益管理装置との間でネットワークを介して伝送されるデータは、機密性に応じて暗号化するステップを含む。

【 0 0 1 3 】

上記構成により、利用者の手元からシステムを制御し、データの入出力を行い、処理結果を表示する方法を提供するものである。

【0014】

又、利用者端末との間でやりとりするデータを圧縮し、暗号化し、かつ利用者毎又は管理対象資産毎に認証キーを付加し、低容量の回線使用下でも大容量データを入出力する利便性とセキュリティを提供するものである。

【0015】

又、利用者毎又は管理対象資産毎に記憶領域を持ち、利用者又は管理対象資産毎に別々の方式や異なる基準に基づく出力結果を抽出して提供するものである。

【0016】

又、地理的に分散あるいは複数になりうる利用者端末側ではなく、集中された拠点に配置されるため、容易な機能改定と維持コストを実現するものである。

【0017】

【発明の実施の形態】

次に、本発明の実施の形態について、添付図面を参照して説明する。

【0018】

＜本実施の形態の資産管理システムの構成例＞

図1は、本発明の一実施の形態のシステムを示すブロック構成図である。

【0019】

図において、1は、利用者又は管理対象資産毎の入出力データを格納及び検索するデータ管理部、2は、データ管理部1及びネットワークからの入力データを処理し出力データを得る計算処理部、3は、利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理部、4は、フロー制御とデータ暗号化とデータ圧縮展開とを行うネットワーク接続管理部であり、これらデータ管理部1と計算処理部2と履歴認証管理部3とネットワーク接続管理部4とで、リスク収益管理装置を構成する。尚、本例ではリスク収益管理装置を構成する各構成要素をネットワーク接続管理部4に接続する構成で示したが、データ管理部1と計算処理部2と履歴認証管理部3がネットワーク上に分散して配置されていても、あるいはLANなどの構内ネットワークで接続されていても構わない。

【0020】

5は、地理的に分散した複数の利用者又は管理対象資産のデータを結ぶネットワーク回線であり、インターネット、公衆回線接続、又は専用ネットワークを含む。6は、システムを制御し、データの入出力を行い、処理結果を表示する利用者端末である。利用者端末6は複数存在し、地理的に散在していて構わない。すなわち、利用者端末6は、金融機関にあっても、一般の個人の所有であっても構わず、誰もが本システムに参入することが可能である。

【0021】

図2は、上記のような本システムを実現するためのハードウェア構成例を示す図である。図2において、図1と対応する要素は同じ参照番号を付与している。

【0022】

図2において、1はデータ管理部であり、資産データが利用者及び／又は管理対象資産毎に管理されて格納されているデータ管理データベース(DB)1aと、そのデータ管理プログラム1bとを含む。2は計算処理部に対応する資産変動などを計算する計算処理プログラム、3は履歴認証管理部であり、利用者単位でその履歴及び認証キーを格納する履歴認証キーデータベース(DB)3aと、履歴認証を実行する履歴認証プログラム3bとを含む。4はネットワーク接続管理部であり、ネットワークを介して送信されるデータを圧縮し、受信されたデータを展開するデータ圧縮展開プログラム4aと、ネットワークを介する通信接続のプロトコル等の実行、及びデータの暗号化／復号を実行する接続応答・暗号化プログラム4bとを含む。これらのデータ及びプログラムは、ハードディスクやフロッピーディスクなどの磁気ディスクや、CD-ROM、CD-RWやDVDなどの光ディスク、メモ리카ード等の大容量の記憶装置に格納されており、主記憶装置21にロードして実行される。

【0023】

リスク収益管理装置側で、7はキーボード装置であり、リスク収益管理装置の起動・停止・監視などの操作を行う。8はディスプレイ装置であり、キーボード装置7の操作に応じてリスク収益管理装置の状態を表示する。21は、上記記憶装置からデータ及びプログラムをロードしたり、計算処理時に一時記憶として使

用される主記憶装置、22は主記憶装置21にロードされたプログラムにより、リスク収益管理装置全体を制御する制御装置、23は計算処理プログラム2に従って特殊な計算を高速で行うように用意された演算装置である。尚、制御装置22と演算装置23は、汎用コンピュータでは1つのCPUで実現されるし、特殊コンピュータでは並列動作する複数のCPUに分配されている。

【0024】

5はネットワーク回線であり、利用者端末6側にはネットワーク接続装置5a、リスク収益管理装置側にはネットワーク接続装置5bが配置されている。

【0025】

利用者端末6において、9は、利用者端末のキーボード装置であり、リスク収益管理装置側に対して、バリュー・アット・リスク（VaR）、リスク・リターン分析、ポートフォリオ最適化などの計算実行、データ転送、結果照会などをコマンド操作したり認証データなどを入力する。10は、利用者端末のディスプレイ装置であり、キーボード装置7の操作に応じてリスク収益管理装置が返した応答及び各種制御表示プログラム15で解析処理された結果を表示する。11は、利用者端末6全体を制御する制御装置、12は、利用者端末上で各種演算処理を行う演算装置である。尚、利用者端末6は誰でも本システムに参入できるように汎用コンピュータが好ましく、一般に制御装置11と演算装置12とは1つのCPUで実現される。

【0026】

20は記憶装置であり、以下のデータ及びプログラムが記憶されている。13はデータ圧縮展開プログラムで、リスク収益管理装置のネットワーク接続管理部4との間で送受するネットワーク回線5を流れるデータの圧縮と展開を行う。14はデータ暗号化プログラムで、リスク収益管理装置のネットワーク接続管理部4との間で送受するネットワーク回線5を流れるデータの暗号化を行う。15は、利用者端末における各種の制御表示を行う各種制御表示プログラムである。16は、ネットワーク回線5を介してデータ管理部1に送られるまで一時滞留する資産データ記憶部である。

【0027】

＜本実施の形態の履歴認証の構成例＞

図 3 は、履歴認証キー DB 3 a の一構成例を示す図である。

【 0 0 2 8 】

利用者端末 6 から送信されたデータには、少なくとも端末 ID、利用者 ID（パスワード等を含む）、履歴認証キーが含まれており、これらに基づき履歴認証キー DB 3 a の端末 ID 3 1、利用者 ID 3 2、履歴認証キー 3 3 を検索して、一致するものを探す。一致するものが無ければリスク収益管理装置は利用者端末 6 からの要求を受付けない。一致するものがあれば、入力データ制限 3 4、計算処理制限 3 5、出力データ制限 3 6 に基づいて、その利用者が利用できる資源及び提供するサービスを制限する。例えば、この制限は、同じ金融機関からか、他の金融機関からか、あるいは一般の顧客からか、更に顧客であれば、取引高や取引継続年月などに基づいて、決定されればよい。尚、端末 ID については、利用範囲を拡大する見地からすると、認証に含まない方が望ましい。

【 0 0 2 9 】

図 3 では、入力データとして A、C、D…が使用され、B の使用が制限されている。計算処理では、コマンド a、b、d が処理されるが、コマンド c の処理はされない。計算結果の内、出力データ I と III は出力（利用者端末に返される）が、出力データ II は出力されない。ここで、特にコマンドは 1 つの処理方式を複数のコマンドに分けて制限すると共に、複数の処理方式から特定の処理方式を選ぶ、あるいは入力データや出力フォーマットに対応して特定の処理方式を選ぶような制限も加えて階層的に制限すると、より汎用性を持ったシステムが構築される。更に、要求される処理方式を持たない場合に、その処理方式を持つ他のシステムを探して、本リスク収益管理装置が他のシステムに対して利用者端末として接続し、計算処理結果を得るように構成すると、資源を共有した汎用システムが構築される。本発明の履歴認証による機密性の確保は、この場合に益々重要な機能となる。

【 0 0 3 0 】

尚、図 3 では、簡略化のために、入力データ、コマンド、出力データ共に、明確に分離されているように示したが、階層構造にしてどの階層までを利用可能に

する方法や、あるいはデータの一部にマスクをしたり、しなかったりを制御する方法、コマンド処理に関しては引数での制限、すなわちプログラム中で使用するパラメータの相違や分岐先の相違などによる制御も考えられる。更に、データの有効桁数の制限、計算での収束幅の制限、出力時にブランクや伏せ字に変更される等の制御による制限も可能である。本例において、このように利用者によって資源の利用やサービスを制限するのは、本システムを一般に公開するに際して、企業秘密や顧客の秘密などの機密データがインターネットなどを介して扱われることを考慮したためであり、機密の信頼性が高まるに応じて公開範囲を広くできるという関連がある。

【0031】

図4は、入力データを管理するデータ管理データベース(DB)1bの概略構成例であり、入力データA, B, C, D…の内容が41乃至44で示されている。尚、図4のように入力データが明瞭に分離されることは少なく、上述した如く、各入力データA, B, C, D…がオーバーラップしているのが普通であり、実際には複雑に階層化されたり索引されたりしてデータベースが構造化されている。又、図4では、計算結果の出力データは示されていないが、出力データはデータ管理データベース(DB)1bに蓄積され、後に入力データとしても使用される。この場合の蓄積は、図3の出力データの制限に関係なく、全ての必要データが蓄積される。

【0032】

図4のように、各データ領域41～44はヘッダとデータとから構成されており、ヘッダ部分には履歴認証キーが、例えば、何時、どの利用者が、このデータを登録したか、あるいはその利用者がこのデータの機密性のレベルや、具体的に誰には見せて良いか、誰には見せてはならないかなどが登録時又は更新時に記述され、上記図3の入力制限と相まって機密性を高めている。尚、データベースの機密性に依じて、図3と図4の履歴認証キーはその一方が使用されるものであってもよい。

【0033】

図5は、計算処理プログラム2の一例を示す図である。

【0034】

図5の例では、コマンドa処理51乃至コマンドd処理54が示されている。図5においても、図4と同様に、各コマンド処理プログラム51～54にはヘッダが設けられ、この処理プログラムを使用可能な条件や、使用する場合の処理精度や処理方法に関わる情報が記述されている。

【0035】

尚、図3の計算処理の制限の仕方は一例であって、例えば計算処理プログラム2での制限はコマンド対応でなく、各プログラムの引数で示され、モンテカルロ法などでの計算回数の制限をしてもよい。プログラムの引数の制御の具体例としては、離散型確率密度関数に準拠したモンテカルロ法と、連続型確率密度関数に準拠したモンテカルロ法とを用意し、プログラムの引数によって、両者の適用相手や範囲を制限するものも考えられる。

【0036】

又、図3では、入力データ、計算処理、出力データの全てに制限を設けたが、出力データのみを制限し内部では必要な入力及び計算を全て行って、データ管理データベース(DB)1bに蓄積しておくようにしてもよい。このような場合には、利用者端末に返される出力データは制限に応じてマスクされ、企業名や顧客名、あるいは提供できないデータが伏せ字に置き換えられたものを返送して表示させるのが、営業効果を生む可能性があり好ましい。

【0037】

＜本実施の形態の資産管理システムの動作例＞

以下、本実施の形態の資産管理システムの動作例を示す。尚、利用者端末6での動作、及びネットワークを介するやりとりや、データ圧縮・暗号化などは、本発明の主要部分ではないので、詳細には説明しない。

【0038】

図6は、本実施の形態のリスク収益管理装置の全体の処理を示すフローチャートである。

【0039】

リスク収益管理装置は、ステップS10で、利用者端末6からのリクエストを

待つ。リクエストを受けると、ステップ S 2 0 で利用者端末 6 からのデータを受信する。この時に、端末や利用者の一次認証や、データの暗号解読と圧縮の展開なども行われる。尚、ここで、暗号化はデータの内容によって、その機密性に対応して異なる暗号化、あるいは機密性の高いものには複数の暗号化を行うなどの処理をするのが好ましい。特に、資産データは外部に漏れることを防ぐ必要があり、企業名や顧客名と共に最も厳しい暗号化が行われる。同様に、返送されるリスク収益管理データに対しても最も厳しい暗号化が行われる。

【 0 0 4 0 】

ステップ S 3 0 に進んで、図 7 で説明する履歴認証処理を行う。この履歴認証処理では、上述の利用者による制限が与えられる。ステップ S 4 0 では、制限をもとに入力データ及び／又は処理コマンドがせされ、図 8 で示すリスク変動・収益の計算処理が行われる。ステップ S 5 0 では、計算結果のリスク変動・収益管理データがリスク収益管理装置から利用者端末 6 に返される。利用者端末 6 はこのリスク収益管理データを表示する。尚、この表示フォーマットは、リスク収益管理装置が利用者端末 6 にダウンロードして提供するものであっても（この場合には、上記利用者への制限が表示フォーマットにも適用される）、利用者端末で独自に開発されたものでも構わない。

【 0 0 4 1 】

図 7 は、図 6 のステップ S 3 0 の履歴認証処理の一例を示すフローチャートである。

【 0 0 4 2 】

まず、ステップ S 3 1 では、利用者端末 6 から送られたデータから、端末 I D や利用者 I D が取得される。上述の如く、端末 I D は使用されない場合も多い。次に、ステップ S 3 2 で、履歴認証キーが取得される。ステップ S 3 3 では、取得された端末 I D や利用者 I D、履歴認証キーに基づいて、利用者の「権限」が取得される（図 3 参照）。ステップ S 3 4 では、この取得された「権限」に変更がなされるかを判断し、変更がなければステップ S 3 6 に飛んで、「権限」を表わすデータを計算処理プログラムに渡す。ステップ S 3 4 で変更ありと判断されれば、ステップ S 3 5 で「権限」を変更して、ステップ S 3 6 で、変更された「

「権限」を表わすデータを計算処理プログラムに渡す。尚、「権限」の変更は、金融機関間の関係や、取引額の変化や取引継続年月の長さ、などに基づいて、し尿レベルの変化に応じて逐次おこなわれる。従って、信用レベルの低下によって「権限」が制限されることもある。又、「権限」を、利用者IDや履歴認証キーに対して固定して、再契約時に利用者IDや履歴認証キーを変更するようにして制御してもよい。

【0043】

図8は、図6のステップS40の計算処理の一例を示すフローチャートである。この例では、入力データ、計算処理、出力データの全てで制限を行う例を示している。

【0044】

まず、ステップS41で、ステップS30の結果の「権限」データを取得する。ステップS42では、「権限」データに従って入力データを制限する。ステップS43では、「権限」データに従って計算処理を制限する。ステップS44では、上記入力データと計算処理の制限の下で資産変動やリスク管理の計算処理を実行する。ステップS45では、計算結果の内から「権限」データに応じた情報を選択、あるいはマスクして出力する。

【0045】

【発明の効果】

以上説明したように、本発明によれば、地理的に分散した利用者及び管理対象資産のデータを対象とした場合であっても、効率的かつ安全な資産のリスク管理及び収益管理を可能となる。

【0046】

このため、データ量が大きな大手事業法人や顧客情報や信用情報が含まれるなど機密性の高い金融データを扱う金融機関であっても、低コストで開放されたネットワーク回線、例えばインターネット接続を通して資産のリスク管理及び収益管理機能が実現できるようになる。

【0047】

又、バリュー・アット・リスク、リスク・リターン分析、ポートフォリオ最適

化など、個別の方法論において様々な見解や手法の相違が含まれるポートフォリオ理論を適用する場合は、利用者又は管理対象資産毎の履歴認証情報をもとにして別々の方式や異なる基準をあたかも異なるシステムを操作したかのように機能提供することができる。

【 0 0 4 8 】

加えて、持続的な機能向上や改定を行う場合も、地理的に分散した利用者端末の側はそのままにしておき、集中して設置されたリスク・収益管理装置の側を修正することで対応ができる。このため機能の維持コストや改定コストが低下する効果がある。

【図面の簡単な説明】

【図 1】

本実施の形態の資産管理システムの構成例を示すブロック図である。

【図 2】

本実施の形態の資産管理システムのハードウェア構成例を示すブロック図である。

【図 3】

本実施の形態の履歴認証キー DB の一構成例を示す図である。

【図 4】

本実施の形態のデータ管理 DB の一構成例を示す図である。

【図 5】

本実施の形態の計算処理プログラムの一構成例を示す図である。

【図 6】

本実施の形態のリスク収益管理装置の処理手順例を示すフローチャートである。

【図 7】

図 6 の履歴認証処理の処理手順例を示すフローチャートである。

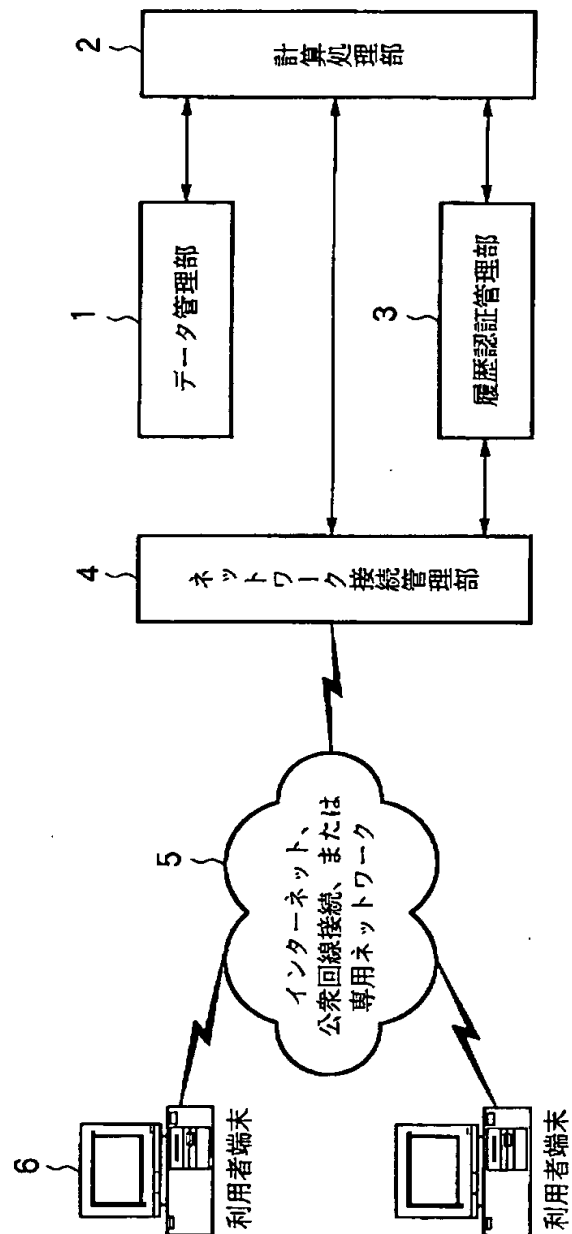
【図 8】

図 6 の計算処理の処理手順例を示すフローチャートである。

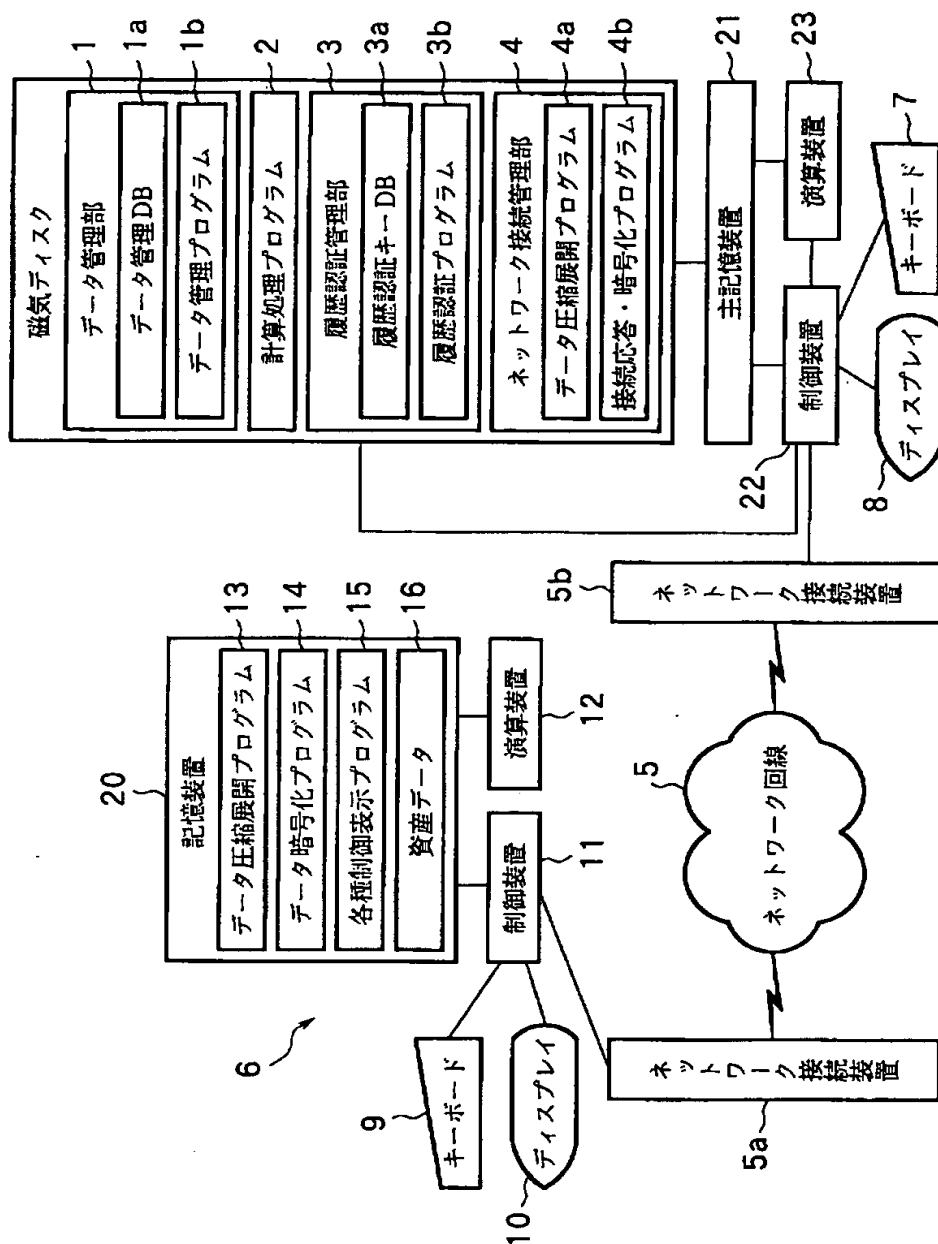
【書類名】

図面

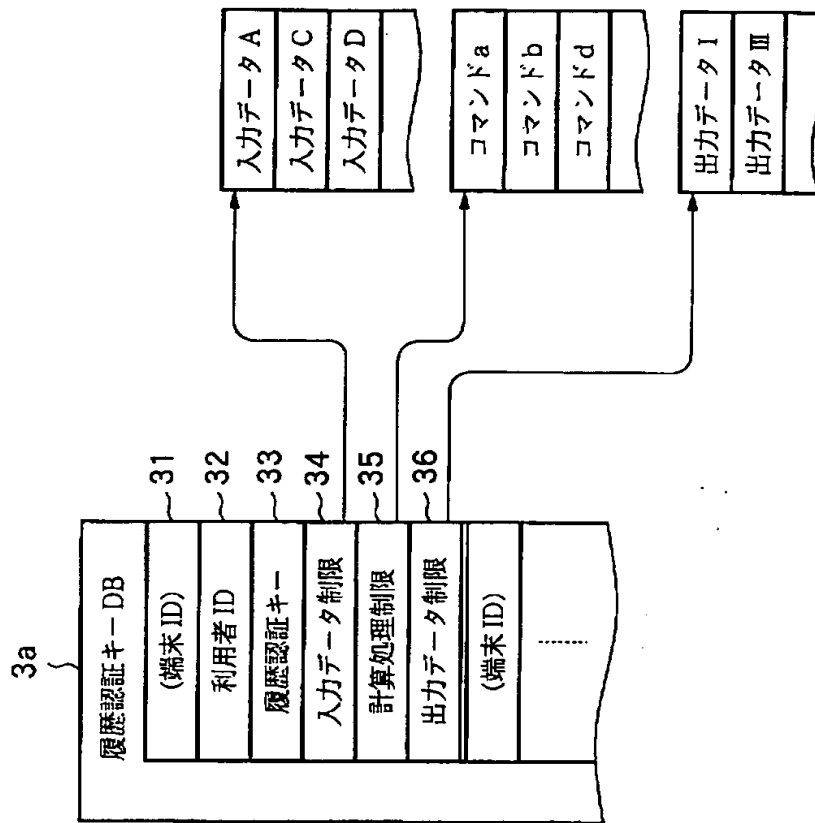
【図 1】



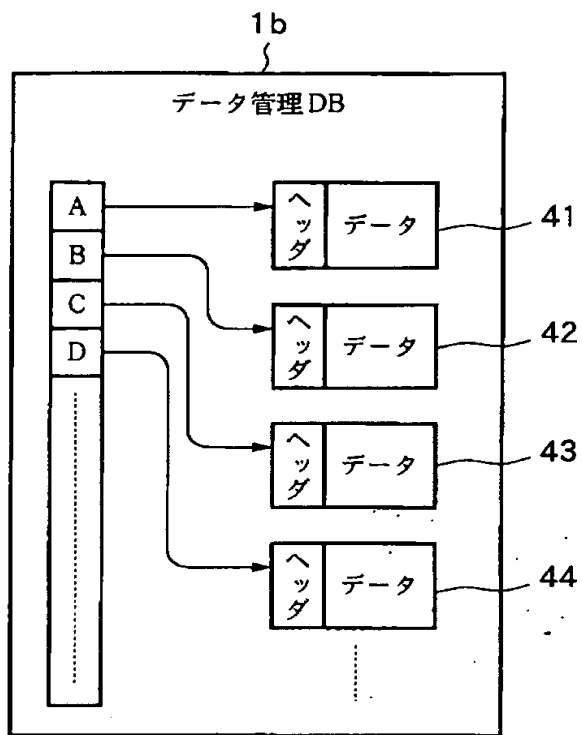
【図 2】



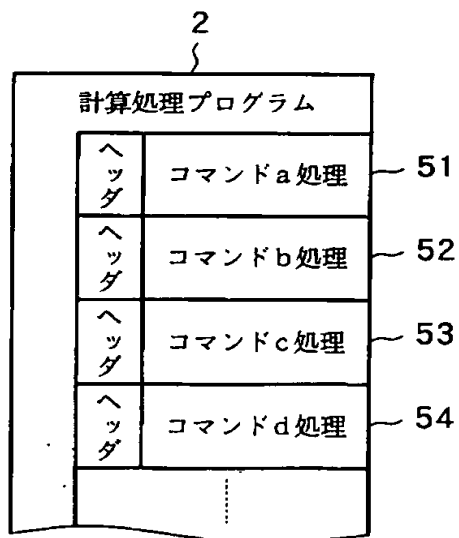
【図 3】



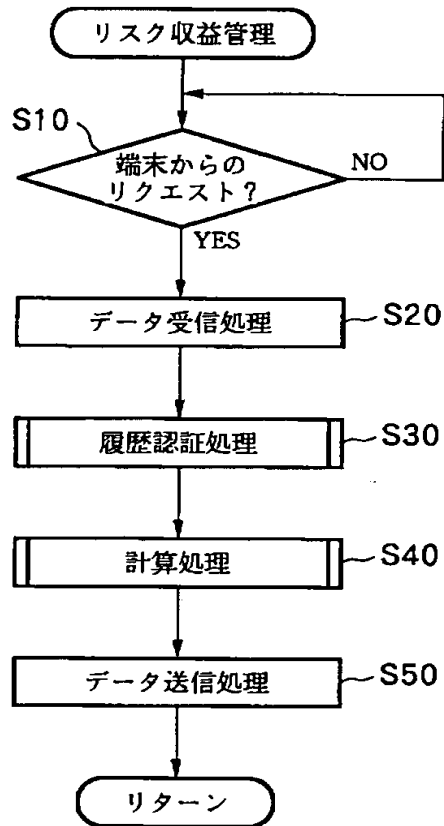
【図 4】



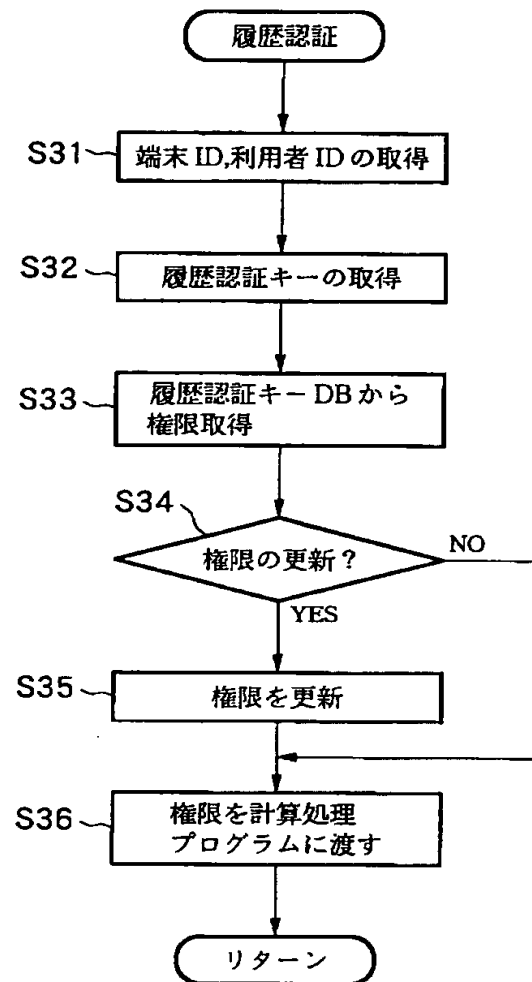
【図 5】



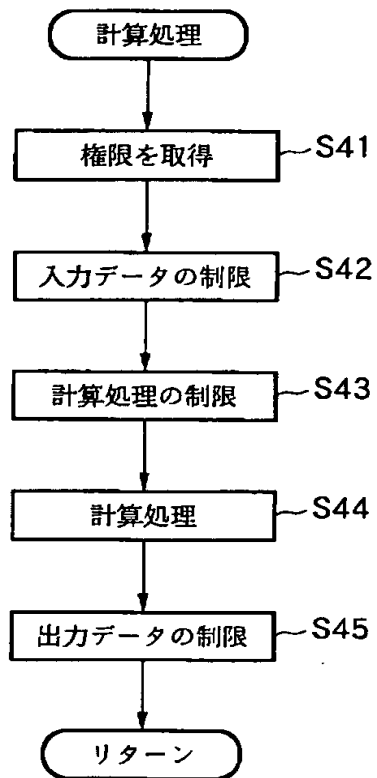
【図 6】



【図 7】



【図 8】



【書類名】 要約書

【要約】

【課題】 インターネット接続に代表される帯域が限定され信頼性と安全性に乏しいネットワーク間通信を利用して、地理的に分散した利用者及び管理対象資産のデータを対象に、利用者又は管理対象資産毎に別々の方式や異なる基準に基づいた資産のリスク管理及び収益管理を行う。

【解決手段】 集中して設置されるリスク収益管理装置と、地理的に分散した利用者端末との間でやりとりするデータを圧縮し、暗号化し、かつ利用者毎又は管理対象資産毎に認証キーを付加し、利用者毎又は管理対象資産毎に別々の方式や異なる基準に基づく出力結果をリスク収益管理装置から利用者端末に流す。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2000-199276
受付番号	50000827238
書類名	特許願
担当官	塩崎 博子 1606
作成日	平成 12 年 7 月 13 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	399070859
【住所又は居所】	東京都文京区本郷 3-4-2-5 ボア本郷 4 階
【氏名又は名称】	ニューメリカルテクノロジーズ株式会社

【代理人】

申請人

【識別番号】	100076428
【住所又は居所】	東京都千代田区紀尾井町 3 番 6 号 秀和紀尾井町 パークビル 7 F 大塚国際特許事務所
【氏名又は名称】	大塚 康徳

【選任した代理人】

【識別番号】	100101306
【住所又は居所】	東京都千代田区紀尾井町 3 番 6 号 秀和紀尾井町 パークビル 7 F 大塚国際特許事務所
【氏名又は名称】	丸山 幸雄

【選任した代理人】

【識別番号】	100115071
【住所又は居所】	東京都千代田区紀尾井町 3 番 6 号 秀和紀尾井町 パークビル 7 F 大塚国際特許事務所
【氏名又は名称】	大塚 康弘

出 願 人 履 歴 情 報

識別番号 [399070859]

1. 変更年月日 1999年 9月 1日

[変更理由] 新規登録

住 所 東京都文京区本郷3-42-5 ボア本郷4階

氏 名 ニューメリカルテクノロジーズ株式会社